Changes in the Claims

1 - 5 (canceled))

6.(currently amended) A method for securely changing an existing password associated with a user identifier (userid) on a host computer to a new password, wherein said passwords enable a user associated with said userid at a local computer to access information on said host computer across a network; said method comprising the steps of:

sending, by the local computer, the userid and a first nonce to the host computer;

replying, by the host computer to the local computer, with a second nonce;

generating, by the local computer, a first digest of the userid and the existing password and a second digest of the userid and the new password;

creating, by the local computer, an authentication token and an authentication token mask wherein said authentication token ~~si~~ is a hash function of the first digest, first nonce and second nonce, and said token mask is a hash function of the second digest, first nonce plus a predetermined value and the second nonce;

generating, by the local computer, a protected digest by ~~exclusive-or'ing~~ exclusive-oring the second digest with the token mask;

sending, by the local computer to the host computer, the userid, authentication token and the protected digest;

verifying, by the host computer, the validity of the authentication token; and,

accepting the new password to replace the existing password if the authentication token is valid.

7 - 9 (canceled)

10.(currently amended) A computer program product for securely changing an existing password associated with a user identifier (userid) on a host computer to a new password, wherein said passwords enable a user associated with said userid at a local computer to access information on said host computer across a network; said ~~method~~ computer program product comprising ~~the steps of~~:

computer readable programming ~~means~~ for sending, by the local computer, the userid and a first nonce to the host computer;

computer readable programming ~~means~~ for replying, by the host computer to the local computer, with a second nonce;

computer readable programming ~~means~~ for generating, by the local computer, a first digest of the userid and the existing password and a second digest of the userid and the new password;

computer readable programming ~~means~~ for creating, by the local computer, an authentication token and an authentication token mask wherein said authentication token is a hash function of the first digest, first nonce and second nonce, and said token mask is a hash function of the second digest, first nonce plus a predetermined value and the second nonce;

computer readable programming ~~means~~ for generating, by the local computer, a protected digest by ~~exclusive-or'ing~~ exclusive-oring the second digest with the token mask;

computer readable programming ~~means~~ for sending, by the local computer to the host computer, the userid, authentication token and the protected digest;

computer readable programming ~~means~~ for verifying, by the host computer, the validity of the authentication token; and,

computer readable programming ~~means~~ for accepting the new password to replace the existing password if the authentication token is valid.

11.(currently amended) A computer program product as claimed in claim 10 wherein said first and second digests are calculated by performing a hash function of the userids and respective passwords.

12.(currently amended) A computer program product as claimed in claim 10 or 11 wherein said hash function is a ~~collision-resistent~~ collision-resistant, one-way hash.